Metrics-Based Risk Assessment and Management of Digital Forensics in Acquisition Domain

M. Sahinoglu* (MeSa@aum.edu), Stephen Stockton, Robert Barclay and Scott Morton

Informatics Institute, AUM, Montgomery, AL 36124-4023

STATEMENT OF RESEARCH ISSUE/RESULTS (50 words or less)

Driven by the ubiquity of interconnectivity and unavoidable escalation of cyber-criminality in the government and defense industry; DF is an increasingly salient component of the defense acquisition process. To address this undeniable problem, current proposal develops an automated strategy and metric-centric approaches to risk assessment and management within acquisition domain.

PUBLIC PURPOSE (200 words or less)

The assessment and management of information risk is a critical part of operating enterprise applications and Information Technology Systems. While there are many approaches to assessing and managing DF risk (Kim & In, 2008), managers typically focus on the ITS, functionality and often neglect the other aspects of testing and security. Additionally, once all risks are identified, formulating a cost-optimized solution to mitigate undesirable risks to a tolerable level is often taken as an ad-hoc process. Digital Forensics risk arises, for example, when personnel lack the proper tools to conduct investigations, fail to process evidentiary data properly, or do not follow accepted protocols and procedures. Assessing and managing DF risk is the ultimate goal of this proposal. The Offerors implement a Digital Forensics Risk Meter concept, based on a series of questions designed to assess qualified respondents' perceptions of Digital Forensics risk. Based on the expert responses, a DF risk index will be calculated. Numerical and/ cognitive data will be collected to calculate the quantitative risk index for acquisition-related applications. The outcomes will not only present a quantitative model but also provide cost-optimized game-theoretic analysis on how to mitigate an undesirable risk to a user-determined tolerable-level**.**

TECHNICAL CONCEPT

(1)A description of proposed research and associated risk areas:

Digital Forensics risk (digital evidence assessment subject to given standards) is to be quantified using a Risk Meter algorithm for calculating risk indices, and implemented for the domain of Defense Acquisition Process. Assessing and quantifying digital forensics risk is the goal of this paper. Forensics that derives from ancient Roman "forum" where post-war discussions are held to outline vulnerabilities is as old as humanity. A Digital Forensics Risk-Meter's automated and algorithmic software based on a series of learned questions designed to assess expert personnel's perceptions of digital forensics risk will be utilized. Based on the responses, a digital forensics risk index will be calculated. Amran et al proposed *Network Forensics Readiness* in 2008; Jones & Valli wrote on building a DF lab in 2011. The Digital Forensics Risk-Meter presented whereas in this proposal will provide objective, automated, dollar-based risk mitigation advice for interested parties such as investigators, administrators, and officers of the court to minimize digital forensics risk. See Figure 1 for the decision tree diagram to assess; then Figure 2's advice column for mitigation from Figure 3's sample respondents' ranked outputs tabulated. This proposal generates an index to translate the appropriate protocols and procedures, by entering in the XML survey-warehouse the right-queries toward the assessment and management model. Hence, legal standards of proof and admissibility are met to reach a conclusive index to mitigate.

(2)A statement on how the proposed effort is relevant to the research areas :

The proposed research proposal will be targeting *risk (assessment and) management* regarding public procurement policy and management in defense (or similar) acquisition systems.

(3)Research Questions and Objectives:

Q1) What is the establishment's current risk status expressed by a summary index of the digital communications (internet, ftp etc.) related network's unwanted breaches.

The *objectiv*e is to estimate a probabilistic risk index based on evidential responses.

Q2) What are the bottlenecks, problems and critical issues that cause the establishment to waste budgetary and human resources detected due to lower-than-standard practice by the outcomes obtained; such as the enterprise may experience 25% more Digital Forensics breaches than the set-up standards on an annual basis?

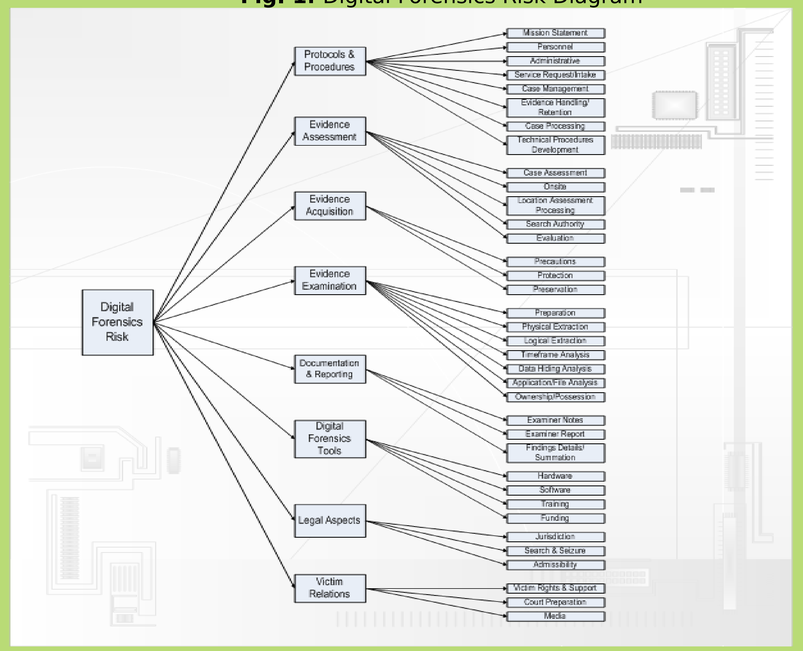
The *objective* is to specify the problem points that one needs to mitigate to improve the digital communication system void of illegal and unethical breaches.

Q3) Can the establishments specify a quasi-complete body of related vulnerabilities, threats and countermeasures to work towards the assessment of a quantifiable risk, after which a consequential dollar-based risk management remediation is pursued to make good following a related set of investments defined as countermeasures to implement.

The *objective* is to provide guidance for cost-effective budgetary allocation plan to verify that the improvements are made. A second round of remediation efforts can be executed provided an extended budget. New vulnerabilities and threats will be countermeasured.

(4) A) Methodology and B)Conclusions: **A)**The project proposal will employ probabilistic and game-theoretic linear programming techniques to assess and manage DF risk. See Table 1 for a linear system of governing equations used within the body of the Security–Meter's software for the game-theoretic algorithm

Fig. 1: Digital Forensics Risk Diagram



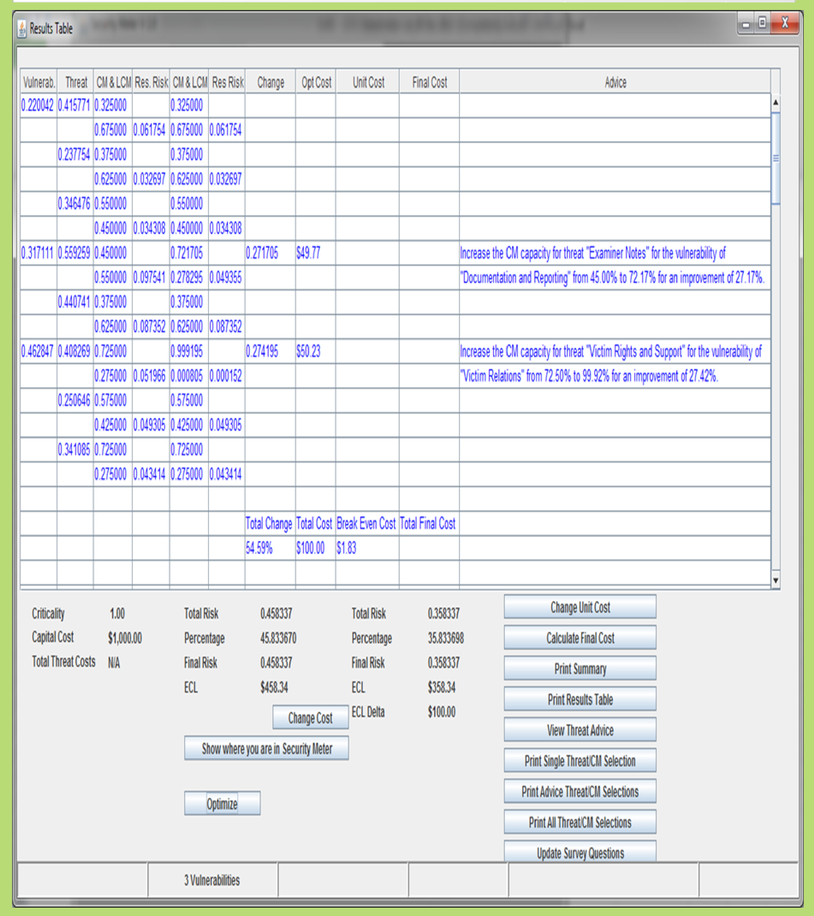


Fig. 2: Median Digital Forensics Risk Meter (Sample) Results from ALABAMA forensics legal and law enforcement (police) departments mitigated to 35.83% from 45.83%

Fig. 3 Survey results for the Risk Meter study, ranked within and overall; where Median: 45.83 (ECSO8) and Average: 44.73%

Respondent Results Tabulations

Survey Taker	Residual Risk %	Ranked Overall (out of 27)	Remarks
AFIT1	52.47	6th	2nd out of 4 within AFIT
AFIT2	49.90	9th	3rd out of 4 within AFIT
AFIT3	52.71	5th	1st out of 4 within AFIT
AFIT4	47.64	10th	4th out of 4 within AFIT
AUPD1	31.15	26th	7th out of 7 within AUPD
AUPD2	39.67	20th	5th out of 7 within AUPD
AUPD3	50.02	8th	1st out of 7 within AUPD
AUPD4	36.98	21st	6th out of 7 within AUPD
AUPD5	44.59	16th –OVERALL AVERAGE	4th out of 7 within AUPD
AUPD6	46.06	13th	3rd out of 7 within AUPD
AUPD7	47.06	11th	2nd out of 7 within AUPD
ECSO1	51.80	7th	5th out of 9 within ECSO
ECSO2	46.66	12th	6th out of 9 within ECSO
ECSO3	56.94	2nd	2nd out of 9 within ECSO
ECSO4	57.67	1st	1st out of 9 within ECSO
ECSO5	54.87	3rd	3rd out of 9 within ECSO
ECSO6	41.36	19th	9th out of 9 within ECSO
ECSO7	54.84	4th	4th out of 9 within ECSO
ECSO8	45.83	14th OVERALL MEDIAN	7th out of 9 within ECSO
ECSO9	45.01	15th	8th out of 9 within ECSO
OPD1	35.00	23rd	4th out of 7 within OPD
OPD2	42.56	18th	2nd out of 7 within OPD
OPD3	44.35	17th	1st out of 7 within OPD
OPD4	33.39	25th	6th out of 7 within OPD
OPD5	28.23	27th	7th out of 7 within OPD
OPD6	34.39	24th	5th out of 7 within OPD

Min COLLOSS (Column loss), s. t. (subject to):

$CM_{11} < 1$ (1), $CM_{12} < 1$ (2), $CM_{13} < 1$ (3), $CM_{21} < 1$ (4), $CM_{22} < 1$ (5), $CM_{31} < 1$ (6),
$CM_{32} < 1$ (7), $CM_{33} < 1$ (8), $COLLOSS < 1$ (9)
$CM_{11} > 0.675$ (10), $CM_{12} > 0.475$ (11), $CM_{13} > 0.725$ (12),
$CM_{21} > 0.725$ (13), $CM_{22} > 0.725$ (14),
$CM_{31} > 0.675$ (15), $CM_{32} > 0.675$ (16), $CM_{33} > 0.675$ (17),
$0.09148\, CM_{11} - 1 COLLOSS < 0$ (18), $0.05231\, CM_{12} - 1 COLLOSS < 0$ (19),
$0.07629\, CM_{13} - 1 COLLOSS < 0$ (20), $0.17734\, CM_{21} - 1 COLLOSS < 0$ (21),
$0.13966\, CM_{22} - 1 COLLOSS < 0$ (22), $0.18896\, CM_{31} - 1 COLLOSS < 0$ (23),
$0.11601\, CM_{32} - 1 COLLOSS < 0$ (24), $0.15787\, CM_{33} - 1 COLLOSS < 0$ (25),
$0.09148\, CM_{11} + 0.05231\, CM_{12} + 0.07629\, CM_{13} + 0.17734\, CM_{21} + 0.13966\, CM_{22} + 0.18896\, CM_{31} + 0.11601\, CM_{32} + 0.15787\, CM_{33} > 1 - 0.3583 = 1 - 0.3583 = 0.6417$ (26)

Table 1: Set of constrained linear equations for Table 1's median to attain a risk mitigated to 35.83% from an undesirable 45.83% inspired by Figure 2; where Total # Constraints = 3 * #Selected Threats + 2=3*8+2=24+2=26 along with Objective(Min).

(5) References

Sahinoglu, M. (2007). *Trustworthy Computing*, Hoboken NJ: John Wiley

Kim, D. H., & In, H. P. (2008). Cyber Criminal Activity Analysis Models using Markov Chain for Digital Forensics, Proceedings of the 2nd International Conference on Information Security and Assurance, ISA 2008. 2008. p. 193-198 4511561, Busan, Korea, Republic of

Amran, A. R., Phan, R. C. W., & Parish, D. J. (2009). Metrics for Network Forensics Conviction Evidence, ICITST Internet Technology and Secured Transactions, International Conference for IEEE, p. 1-8, DOI: 10.1109/ICITST.2009.5402640

Jones, A. & Valli, C. (2011). Building a Digital Forensic Laboratory: Establishing and Managing a Successful Facility, Butterworth-Heinemann.

Sahinoglu, M., Cueva-Parra, L., & Ang , D. (2012) Game-theoretic computing in risk analysis, *WIREs Comput. Stat*, doi: 10.1002/wics, 1205. http://authorservices.wiley.com/bauthor/onlineLibraryTPS.asp?DOI=10.1002/wics.1205&ArticleID=961931

Sahinoglu, M., Stockton, S., Morton, S., Barclay, R., Eryilmaz, M. (2014). Assessing Digital Forensics Risk: A Metric Survey Approach, SDPS Conference Proceedings (Theme: Smart Innovative Societies), 19th International Conference on Transformative Science, Engineering Business and Social Innovation; Sarawak, Malaysia. Available at http://www.swinburne.edu.my/sdps2014

Sahinoglu M, Morton, S., Stockton. S., Barclay, R. (2016). Metrics-Based Risk Assessment and Management of Digital Forensics, DAU (Defense Acquisition University) Hirsch Paper Competition 2nd Prize Winner, to be published in Defense ARJ, April 2016.